Software Maintenance Release Note

Version 89275-02 for AT-8900 and AT-9900 series switches

Introduction

This release note lists the issues addressed and enhancements made in version 89275-02 for Software Release 2.7.5 on existing models of AT-8900 and AT-9900 series switches. File details are listed in Table 1.

Table 1: File details for version 89275-02.

Base Software Release File	89-275.rez
Release Date	November 25 2005
Compressed File Name	89275-02.rez
Compressed File Size	4480884 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.7.5 for AT-9900, AT-8900, SwitchBlade, AT-9800, AT-8800, Rapier, Rapier i, AT-8700XL, and AT-8600 Series Switches and AR400 and AR700 Series Routers (Document Number C613-10454-00 REV A) available from *www.alliedtelesyn.com*.
- AT-8900 series switch Documentation Set for Software Release 2.6.2 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- AT-9900 series switch Documentation Set for Software Release 2.6.6 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.com*.

WARNING: Using a maintenance release for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Enabling and installing this Release

To use this maintenance release you must have a base release license for Software Release 2.7.5. Contact your distributor or reseller for more information.

To enable this release and install it as the preferred release, use the commands:

```
enable rel=89275-02.rez num=2.7.5
set install=pref rel=89275-02.rez
```

Features in 89275-02

Maintenance release 89275-02 includes the following enhancements and resolved issues:

Level 1

No level one issues.

Level 2

CR00008262 Module: OSPFv2 Level:2

Modifying the deadInterval, helloInterval, pollinterval, transitDelay, rxmtinterval, authentication, password, or boost1 parameters of the SET OSPF INTERFACE command used to caused the router to drop neighbour adjacencies. These parameters now can be modified without dropping the neighbour relationships.

Modifying the stubmetric and authentication of SET OSPF AREA command caused the router to drop the neighbour adjacencies on the area. These parameters now can be modified without dropping the neighbour relationships.

Modifying the effect of the SET OSPF RANGE command used to caused the router to drop the neighbour adjacencies on all the interfaces of the range. This parameter now can be modified without dropping the neighbour relationships.

CR00008325 Module: USER Level: 2

If users were defined on a RADIUS server for the purpose of 802.1x or firewall authentication, then these users were also given console login rights with user privilege. The default behaviour has been changed so that console login is only authorised through explicitly setting the service-type attribute of the RADIUS record to Login (for User Privilege), NAS prompt (for Manager privilege), or Administrative (for security officer privilege).

CR00008329 Module: STP Level: 2

If ports that were members of a trunk group were also members of multiple VLANs, and those VLANs were spread across more than one STP instance, the STP states of the ports were not always being set correctly.

CR00008391 Module: NAT Level: 2

An issue existed in IP NAT when creating a new session for a packet destined for an IP address that had been dynamically allocated to a private IP address. The session created would NAT the destination address to the source address of the packet instead of the private IP address.

This issue has been resolved.

CR00008691 Module: DHCP4 Level: 2

Previously, a DHCP received by the server from a client which it should have had no knowledge about was acted on by that server and a NAK was sent to the client. This interfered with any responses from the actual server which was responsible for this client. This delayed the time it took the client to establish an IP address from the correct server. This is now corrected and the server now behaves in a manner which is compliant with the RFC, resulting in faster establishment of an IP address using DHCP under these conditions.

CR00008737 Module: OSPFv2 Level: 2

When the router was acting as an NSSA ASBR it was not setting the forwarding address in Type 7 LS update, therefore Type 7 LSAs were not being translated.

This issue has been resolved.

CR00009236 Module: BGPv4 Level: 2

BGP distribution of routes to another peer when learnt from a peer was very slow.

This issue has been resolved.

CR00009242 Module: LACP Level: 2

Some enhancements have been made so that:

1.When any of the ports in a trunk group is disconnected, there will be no momentary communication interruption.

2.When the second last LACP trunk port is disconnected, there will be no momentary communication interruption.

3.An issue has been resolved where LACP was randomly setting the switch port to STP BLOCK.

CR00009313 Module: PORT AUTH Level: 2

When a switch port was disabled using the DISABLE SWITCH PORT command, the MAC address of the authorised supplicant on the port remained in the FDB table. The supplicant's MAC address is now removed when the port is disabled. This has been resolved on both single- and multi-supplicant mode.

When portauth was disabled by using the DISABLE PORTAUTH command, the supplicant MAC address in the switch filter was not removed. This has been resolved and all MAC addresses added by portauth internally are deleted when the supplicant is removed or unauthorised. Also the same behaviour in PURGE PORTAUTH PORT, SET PORTAUTH PORT DEFAULT, DISABLE PORTAUTH PORT and RESET PORTAUTH PORTMULTIMIB commands has been fixed in both 802.1x and MAC-based port authentication.

CR00009331 Module: OSPF Level: 2

Previously, the command SET IP ROUTE PREFERENCE would reset the OSPF neighbour connection, now this reset is no longer required.

This issue has been resolved.

CR00009361 Module: IPv4 Level: 2

If the router received a stream of IPv4-encapsulated IPv6 packets, a memory leak could occur if no IPv6-over-IPv4 tunnel was configured.

This issue has been resolved.

CR00009405 Module: BGP4 Level: 2

Previously, when BGP recorded a BGP peer route with nexthop = 0 (a rare case), it would enter it into its next hop list table but then would fail next time it checked the integrity of the data on this list while reviewing the list after a link state change.

This issue has been resolved.

CR00009409 Module: SWITCH Level: 2

In rare circumstances it was possible for the SFP LEDs to apparently freeze.

This issue has been resolved.

CR00009421 Module: QoS Level: 2

When the command SET QOS was issued with parameters to set multiple flow groups to the same action rule, the switch would reboot.

When the command SET QOS was issued for multiple traffic classes to the same action, the switch would reboot.

These issues have been resolved.

CR00009492 Module: SWITCH Level: 2

The CREATE CONFIGURATION and SHOW CONFIGURATION DYNAMIC output for some VLAN commands were output in incorrect order.

This issue has been resolved.

CR00009728 Module: TRIGGER Level: 2

When the switch was rebooted, time based triggers were not being re activated.

This issue has been resolved.

CR00009885 Module: SWITCH Level: 2

When the switch's L2 MAC entry aged out, it wasn't maintaining the correct linkage between L2 MAC and L3 IP entries.

This issue has been resolved.

CR00009963 Module: STP Level: 2

When multiple STP instances were configured on a switch with multiple VLANs and a topology change happened on one STP instance, the learned IP table entries on ports that did not belong to the STP instance in question were left unaffected.

This issue has been resolved.

CR00010030 Module: PORT AUTH Level: 2

In Multi-Supplicant mode, the SET PORTAUTH PORT command cleared the FDB entries even though there was no configuration change by the command. This has been resolved now, and the MAC address of the authorised supplicant will not be removed from the FDB table by the SET PORTAUTH PORT command.

CR00010043 Module: BGPv4 Level: 2

Previously, the BGP MUILT_EXIT_DISC value was forwarded in update messages to external peers for AS-local routes.

This issue has been resolved.

CR00010053 Module: BGPv4 Level: 2

In BGP, the Nexthop was not being updated correctly if the link to a Nexthop went down and an alternate Nexthop for the same route existed.

This issue has been resolved.

CR00010070 Module: Level: 2

Previously, the command 'SHOW SWITCH FDB' was not correctly utilising the VLAN and PORT parameters.

This issue has been resolved.

CR00010071 Module: Level: 2

Previously, the order of the BGP commands in "CREATE CONFIG=" or "SHOW CONFIG DYN=BGP" was incorrect.

This issue has been resolved.

CR00010166 Module: PORT AUTH Level: 2

When a the SUPPLICANTMAC parameter was used in the RESET PORTAUTH[=MACBASED] PORT command to specify the supplicant to reset, all supplicants would be removed from the switch FDB (Forwarding DataBase) regardless. This issue has now been resolved, so that only the specified supplicant is removed from the switch FDB.

This issue has been resolved.

CR00010168 Module: BGPv4 Level: 2

When BGP damping was enabled, withdrawn routes were not correctly having their damping history maintained until they either returned or the damping history timed out and they were deleted.

This issue has been resolved.

CR00010169 Module: BGPv4 Level: 2

When a route's attribute was updated in the BGP route table, a damping record was not created in the history.

This issue has been resolved.

CR00010202 Module: SWI DRIVER Level: 2

Previously, the polarity was incorrectly showing MDI instead of MDI-X in the output of "SHOW SWITCH PORT=x".

This issue has been resolved.

CR00010219 Module: RADIUS Level: 2

When using telnet login authentication with a Radius-backup User (RBU), the switch could reboot.

This issue has been resolved.

CR00010223 Module: OSPF Level: 2

BGP routes imported into OSPF are now advertised in external LSAs as metric type 2.

CR00010240 Module: OSPF Level: 2

When a default route was imported into OSPF (e.g. from BGP), the OSPF DEFROUTE parameter setting was not being checked.

This issue has been resolved so that if that parameter is set to OFF, the default route is not imported into OSPF.

CR00010241 Module: OSPF Level: 2

Previously, the output created from "create config=" or "show conf dyn=OSPF" would produce a "SET OSPF TYPE=2" when it should have produced "SET OSPF TYPE=1"

This issue has been resolved.

CR00010318 Module: RIP Level: 2

If RIP was configured to send RIP version 2, then multiple routes to the same destination with different masks were not being correctly included in the RIP response or trigger response messages. Only the best route was sent.

This issue has been resolved.

CR00010365 Module: DHCPv4 Level: 2

When creating a dhcp range, the help text invoked by the "?" offered the values 0 to 4294967295. However, the valid range of values is actually 0 to 256.

This issue is now resolved.

CR00010392 Module: GRE Level: 2

Previously, a system reboot could occur if a ping packet was routed out via a local IP interface.

Now, a local IP interface is no longer a valid value for the INTERFACE parameter of the ADD IP ROUTE and ADD IP ROUTE TEMPLATE commands.

CR00010521 Module: BGPv4 Level: 2

There was an issue whereby BGP withdrew a route incorrectly when a better route was available in the IP route table.

This issue has been resolved

CR00010539 Module: FILTER Level: 2

The switch or router sometimes incorrectly bypassed the fast flow packet forwarding mechanism un-necessarily if any of the interface(s) used for forwarding packets were associated with a filter with a variable field pattern(s), such as filtering by TCP session or ICMP code and types. This caused degradation in packet forwarding by the software based routing engine. The issue does not affect forwarding done in hardware.

This issue has been resolved.

CR00010606 Module: OSPF Level: 2

Default routes imported into OSPF were not being advertised in AS external LSAs when the DEFROUTE parameter was set to OFF. If they were advertised previously, they were removed.

This issue has been resolved.

CR00010631 Module: IPv4 Level: 2

When the switch received the first multicast data packet for a given multicast destination address, after learning group membership on a downstream interface. The switch was taking some time to update the software forwarding table for the multicast group, hence may have failed to forward the first packet.

This issue did not affect a multicast group that was already learnt by the routing protocol, nor did it affect a multicast group which had been added to the hardware multicast group table.

This issue has been resolved.

CR00010661 Module: BGPv4 Level: 2

In some network configurations, BGP was withdrawing routes when disabling an importing protocol.

This should not have occurred if there were still other importing protocols that had more preferred routes to the same destinations.

This issue has been resolved.

CR00010727 Module: BOOTP Relay Level: 2

Previously with BOOTP relay, Option82 information added by another switch was sometimes incorrectly used to update the switch's ARP table.

This issue has been resolved.

CR00010805 Module: Level: 2

Hardware tables were being corrupted when a classifier was modified through the SET command, if the classifier was being used by one of the existing hardware filters.

This issue has been resolved.

CR00010852 Module: IPv4 Level: 2

When changing a parameter for a pre-defined local interface using the SET IP LOCAL command, although the change was completed, an inappropriate error message was output.

Also, the command required an IP address to be specified, even if the IP address of the interface was not being changed. If the same IP address was given, then the command incorrectly failed with an error message.

These issues have been resolved.

CR00010989 Module: FIREWALL Level: 2

With TRUSTPRIVATE=NO on the private interface and two or more policies configured, the firewall caused a system reboot when a node from the private interface tried to connect to the firewall with TCP protocol.

This issue has been resolved.

CR00011002 Module: TCP Level: 2

When loading a file using the HTTP method, occasionally the file would not load if too many out of sequence TCP packets were received.

This issue has been resolved.

CR00011068 Module: SSL Level: 2

Previously, there was a memory corruption issue in the SSL client and server implementation.

This issue has been resolved.

CR00011142 Module: PPP Level: 2

PPPoA frames with padding were incorrectly being silently discarded.

This issue has been resolved.

Level 3

No level three issues.

Level 4

CR00007462 Module: SWK Level: 4

The output of "show switch portsx count" was misaligned.

This issue has been resolved.

Enhancements

CR00010160 Module: BGPv4

Changes to the log system to incorporate 5 new logs:

14 10:24:24 5 BGP BGP 00012 BACKOFF failed to register Lower threshold observer 85%

13 13:27:26 5 BGP BGP 00013 BACKOFF failed to set Upper notification threshold to True

13 13:36:19 5 BGP BGP 00014 BACKOFF failed to set Lower trigger threshold to 15%

13 14:08:51 5 BGP BGP 00015 Consecutive BACKOFF limit reached 20. Disabling Peers

13 14:08:57 5 BGP BGP 00016 Lower BACKOFF threshold reached. Initiating Upper threshold 15%

Implementation of 2 new commands:

```
enable bgp backoff

disable bgp backoff
```

Alteration of the functionality of the "set bgp backoff " command to allow a "low" parameter

E.g. "set bgp backoff low=x" where "x" is between 15 and 99.

Addition of a new sub-command to the "show bgp memlimit" command. This now contains the parameter "bgp".

E.g "show bgp memlimit bgp"

CR00009993 Module: SWITCH

Functionality has been added to enable or disable GBIC / SFP ports electrically or logically, by issuing the respective commands. Disabling ports electrically would mean that the optics for the respective ports can be turned ON or OFF. Logical disabling would indicate that the optics (physical link), remains ON while the ports are disabled at a logical level.

Implementation of a new command parameter:

link = enable/disable

E.g. “ena swi port = x link = enable”

```
/* Show the current status of a GBIC port on the switch
*/

Manager sh swi po=13

Switch Port Information

-----------------------------------------------------

   Port ........................13

   Description .................-

   Status ......................ENABLED

   Link State ..................Up

/* Do a Logical disable */

Manager disable swi po=13

Info (1087003): Operation successful.

/* Show the status of the switch after the electrical
disable */

Manager sh swi po=13

Switch Port Information

-----------------------------------------------------
```

```
   Port ......................13

   Description ...............-

   Status ...................ENABLED <== Optics are ON

   Link State ...............Down

/* Do an enable */

Manager enable swi po=13

Info (1087003): Operation successful.

/* Show the status of the switch after the enable */

Manager sh swi po=13

Switch Port Information

----------------------------------------------------

  Port .....................13

  Description ...............-

  Status ...................ENABLED <== Optics still ON

  Link State ...............Up

/* Do an electrical disable */

Manager disable swi po=13 link=disable

Info (1087003): Operation successful.

/* Show the status of the switch after the electrical
disable */

Manager sh swi po=13

Switch Port Information

----------------------------------------------------

  Port ......................13

  Description ...............-

  Status ...................DISABLED <== Optics go OFF

  Link State ...............Down

/* At this point the optics also get disabled */

/* Do an enable */

Manager enable swi po=13
```

```
Info (1087003): Operation successful.

/* At this point the optics get enabled */

/* Show the status of the switch after the enable */

Manager sh swi po=13

Switch Port Information

------------------------------------------------------

  Port .......................13

  Description .................-

  Status ......................ENABLED <== Optics go ON

  Link State ..................Up
```